République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université d'Ibn Khaldoun – Tiaret

Faculté des Mathématiques et de l'Informatique

Département Informatique

Thème

Sécurité de vidéo numérique par une approche de chiffrement sélectif

Pour l'obtention du diplôme Master II

Spécialité : Réseaux et télécommunication

Réalisé par : Kherroubi abdelhak

Présenté le 28 Octobre 2020 devant le jury composé de :

Mr.MEBAREK Bendaoud	Université de Tiaret	Président
Mr.MEZZOUG Karim	Université de Tiaret	Examinateur
Mr.OUAMRI Mokhtar	Université de Tiaret	Encadreur

Année universitaire 2019 –2020

Dédicace

Je dédie ce modeste travail :

À tous les membres de ma famille mes parents pour leur soutiencontinu et je leurs souhaite bonne santé et longue vie

À tous mes amis,

À tous mes enseignants qui ont fait leurs possibles pour nous donner le maximum d'informations concernant notre étude

Enfin, à toutes celles et tous ceux qui ont contribué de près ou de loin à l'accomplissement de ce travail.

KHERROUBIABDELHAK

Remerciements

Je remercie, au premier lieu, mon Dieu Allah qui m'a offert et préservé une bonne santé et qui m'a entouré de sa bienveillance et sa grâce.

Je remercie mon encadreur Dr Ouamri Mokhtar de sa méthodologie et l'exactitude de ces précieux conseils.

Je souhaite remercier toutes les personnes qui m'ont aidé d'une façon directe ou indirecte à la réalisation de ce mémoire.Nos remerciements aux membres du jury, d'avoir accepté de juger notre travail.

Merci infiniment

Table des matières

Liste des Figures

Liste des tableaux

ملخص

كان تشفير الفيديو موضوعا الكثير من الأبحاث في السنوات الأخيرة. في هذه الأطروحة ، اقترحنا نهج التشفير الانتقائي لمقاطع فيديو، حيث قمنا بتشفير المعاملات الكمية باستخدام التشفير المتماثل. بالإضافة إلى ذلك ، قمنا بتنفيذ نهجنا وناقشنا النتائج التجريبية المختلفة.

Résumé

Le cryptage vidéo a fait l'objet de nombreuses recherches ces dernières années. Dans ce mémoire, nous avons proposé une approche de chiffrement sélectif pour les vidéos H.264, où nous avons chiffré les coefficients quantifiés par un cryptage symétrique (XOR) . De plus, nous avons implémenté notre approche et nous avons discuté les différents résultats expérimentaux.

Abstract

Video encryption has been the subject of much research in recent years. In this thesis, we proposed a selective encryption approach for H.264 videos, where we encrypted the quantized coefficients using symmetric (XOR) encryption . In addition, we implemented our approach and discussed the various experimental results.

Mots clés: H264, chiffrement sélectif, CABAC, codage vidéo,XOR,compression.

INTRODUCTION GÉNÉRALE

Avec le progrès rapide des différentes technologies multimédia, de nombreuses données multimédia sont générées et transmises dans les domaines médical, commercial et militaire, qui peuvent contenir des informations sensibles auxquelles les utilisateurs ne devraient pas avoir accès ou qui ne peuvent être que partiellement exposées.

La sécurité et la protection de la vie privée sont donc devenues un élément important. Au cours des dernières années, plusieurs algorithmes de chiffrement ont été appliqués pour sécuriser la transmission vidéo. Si un grand nombre de schémas de cryptage multimédia ont été proposés dans la littérature et certains ont été utilisés dans des produits réels, des travaux de cryptanalyse ont montré l'existence de problèmes de sécurité et d'autres faiblesses dans la plupart des schémas de cryptage multimédia proposés.

La conception d'un cryptosystème pour le chiffrement de vidéo repose sur l'étude de processus de compression utilisé et le format de codage adopté.dans ce mémoire on propose une approche de chiffrement sélectif appliqué a une video codée en norme h.264.

Nous avons structuré notre mémoire en quatre chapitres :

Dans le premier chapitre nous parlerons sur les caractéristiques des images et des videos d'une manière générale (Couleur d'espace, format ...etc.), nous décrivons la structure des algorithmes de compression ,et en expliquant les norme jpeg et mpeg .

Dans le deuxième, nous définirons la notion du h.264. Après, nous allons passer aux etapes de codage et décodage de cette notion,en citant quelques profiles du h.264.

Dans le troisième chapitre, nous allons définir le chiffrement moderne, et nous présentons une description et une comparaison entre les méthodes de cryptage et des algorithmes. Puis on va terminer par la securité et le chiffrement de video

Dans le dernier chapitre, on va implémenteret développerune application qui chiffre la vidéo par une approche de chiffrement sélectif , et on cloture par une conclusion.

Chapitre I :

les concepts de base de traitements des vidéos

1. Introduction :

On désigne par " traitement video " toutes les techniques ayant pour but la modification des caractéristiques chromatiques ,des pixels ,et des images bitmap. Puisque la vidéo n'est qu'une séquence d'images animées, nous allons commencer par parler d'image numérique et ses caractéristiques (Couleur d'espace, format ...etc.). Après, nous allons passer à la compression de l'information,de l image ,et de la video.

2. L'image numérique :

Une image numérique est une image composée par des pixels, (picture elements).Chacun ayant une représentation numérique pour sa couleur,son intensité ou son niveau de gris.[1]

- **La définition de l'image** :est le nombre fixe de pixels qui est utilisé pour représenter l'image dans ses deux dimensions
- **La résolution d'une image** : c'est le nombre de pixels par unité de longueur dans cette image.

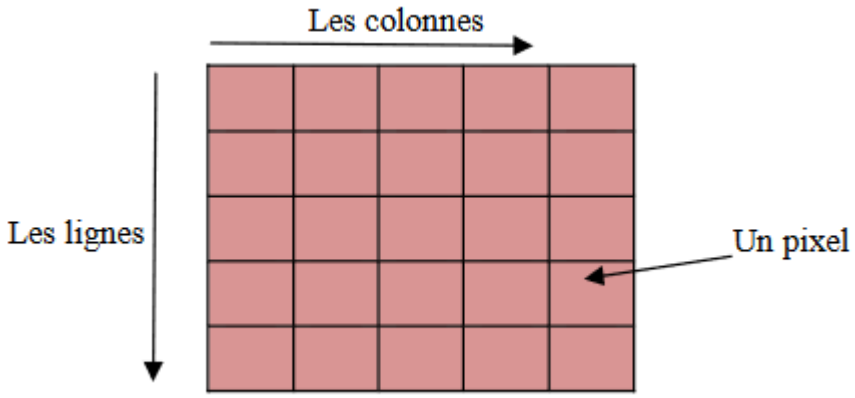


Figure 1 : une image matricielle numérique.

3. Les espaces couleur :

Pour travailler sur des images numériques, On représente donc une image par une fonction à deux variables (les coordonnées), qui renvoie la couleur au point demandé de l'image.

Il existe plusieurs façons de coder les couleurs. La représentation classique d'une image numérique utilise un espace de couleur dit RVB (RGB en anglais).[1]

a) RVB :

Le codage RVB . RougeVertBleu (en Anglais RGB: Red, Green, Blue), est un format de codage des couleurs.

Le codage RVB est sans doute l'espace de couleurs le plus utilisé dans les formats des images JPEG et TIFF, Mais Cette présentation, utilise une grande quantité d'informations.[2]

b) TLS :

Le codage TSL (Teinte, Saturation, Luminosité) ou HSL en anglais (Hue, Saturation, value):

- la teinte(Hue) ou la couleur : rouge, vert, blanc, gris, bleu, vert etc. ;
- la saturation: le degré de pureté, couleur vive (éclatante) ou terne
- la Luminosité(luminance) : l'intensité de lumière incorporée dans la couleur, couleur claire ou sombre.

c) YCrCb(YUV) :

Le codage YCbCr, est utilisé pour la compression d'images et de video. Dans Le format YCbCr, La composante de luminance notée Y fournit une version en niveaux de gris de l'image,tandis que U et V permettent de représenter la chrominance, c'est-à-dire l'information sur la couleur.[2]

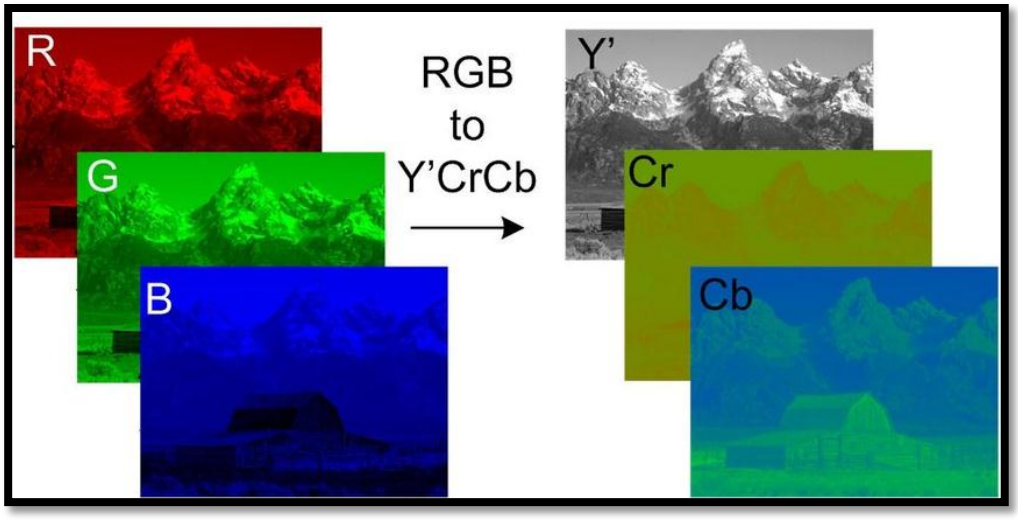


Figure 2:Représentation des couleurs RVBet YCrCb.

4. Echantillonnage de chrominance :

Le sous-échantillonnage chromatique est un type de compression avec perte, qui réduit l'information de couleur dans un signal en faveur des données de luminance. Cela permet de réduire le nombre de bit sans affecter de manière significative la qualité de l'image.[4]

- 4:4:4 vs 4:2:2 vs 4:2:0 :

Explication du format : Le premier chiffre, se réfère à la taille de l'échantillon, Les deux nombres suivants se réfèrent à la chrominance. Ils sont tous deux relatifs au premier nombre et définissent respectivement l'échantillonnage horizontal et vertical.

Exemple :

Résolution de l'image : 1920×1080

PixelsY de résolution : 1920×1080 échantillons, chacun représenté avec une résolution de 8 bits.[4]

- 4:4:4 Cr, Cb : 1920×1080 échantillons, chacun représenté par 8 bits

Nombre total de bits : 1920×1080×8×3=49,766,400bits

- 4:2:0 Cr, Cb : 360×288 échantillons, chacun 8 bits

Nombre total de bits : (1920×1080×8)+(960×540×8×2)=24,883,200bits

- ✓ La version 4:2:0 nécessite deux fois moins de bits que la version 4:4:4.

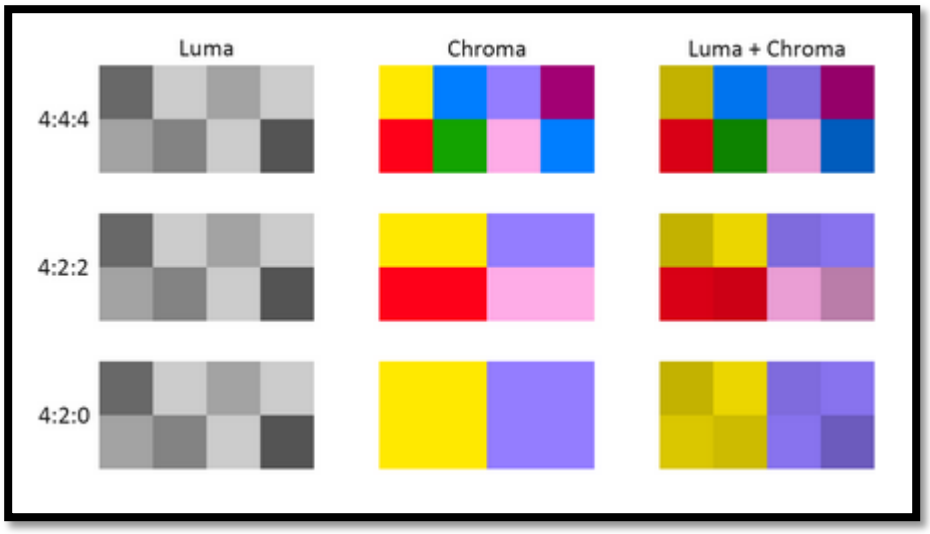


Figure 3 : les formats 4:4:4 vs 4:2:2 vs 4:2:0[4]

5. Vidéo numérique :

Une vidéo numérique est une succession d'images à une certaine cadence. L'oeil humain est capable de distinguer environ 20 images par seconde. avec cette cadence, il est possible de tromper l'œil et de lui faire croire à une image animée. On caractérise la vitesse d'une vidéo par le nombre d'images par secondes (en angla is frame rate), exprimée en FPS (Frames per second, en français (trames par seconde).[3]

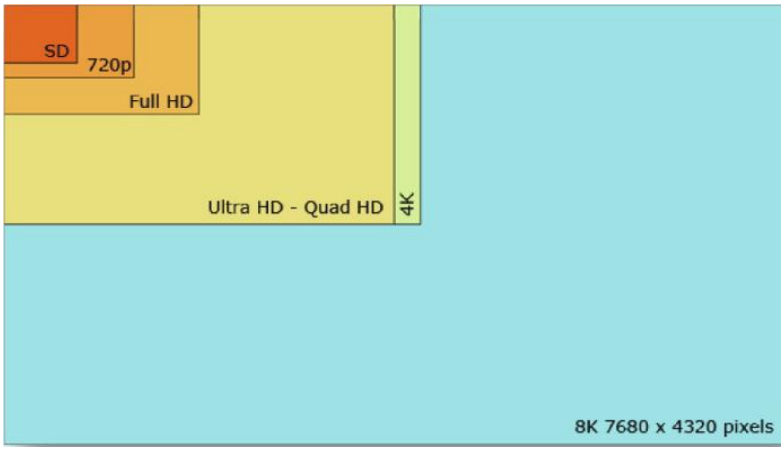


Figure 4:Les formats de la vidéo numérique: de SD au 8K.

6. La compression:

La compression est le processus d'encodage d'une donnée de manière à ce qu'elle consomme moins d'espace que la donnée originale et soit plus facile à transmettre sur le réseau/Internet.

C'est une technique qui réduit la taille des formats de fichiers vidéo en éliminant les données redondantes et non fonctionnelles du fichier vidéo d'origine[8].

- Il existe deux types de compression [3]:

a) la compression avec perte :

Les techniques de compression avec perte impliquent une certaine perte d'informations, et les données qui ont été compressées à l'aide de cette techniques ne peuvent généralement pas être récupérées ou reconstruites exactement.

la compression avec perte ne signifie pas qu'elle supprime les données arbitrairement. Au contraire ,elle utilise une ou plusieurs techniques :

exemple : Echantillonnage de chrominance, DCT et La quantification.

b) la compression sans perte :

Une compression est dite sans perte si les données après décompression sont identiques aux données originelles. Elle élimine seulement les redondances statistiques observée.

La compression sans perte est généralement utilisée pour les applications qui ne peuvent pas accepter de différence entre les données originales et les données reconstruites (aprés la compression et la décompression) [8].

Les algorithmes de compression sans perte sont : le codage de shanon, le codage de Huffman, le codage LZW(Lempel-Ziv-Welch), le codage RLE(run-length encoding) …etc.

7. La compression d'images fixes:

La compression d'une image suit un certain nombre d'étapes.Ces étapes sont illustrées dans le schéma ci-dessous [1]:

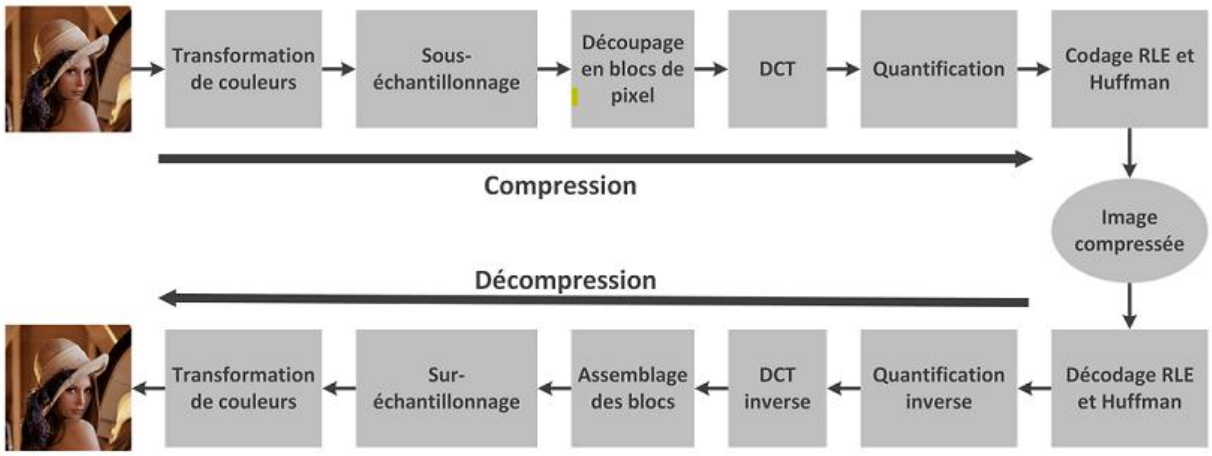


Figure 5 :Étapes de codage typiques utilisées dans la compression MPEG

a) Transformation de couleurs et échantillonnage de chrominance :

La première étape consiste à convertir le modèle initial des couleurs de l'image (souvent RVB) en modèle de type chrominance/luminance (YCrCb),et réduire l'information occupée par l Echantillonnagede chrominance, avec les trois type : 4 :4 :4 , 4 :2 :2 ou 4 :2 :0 .

b) DCT :

Apres Le découpage en bloc de pixels (8×8 ou 4×4), on utilise la technique DCT qui permet d'évaluer l'amplitude des changements d'un pixel à l'autre et d'identifier les hautes et basses fréquences.

Les basses fréquences présentées dans une image sont des zones unies où les couleurs sont proches les unes des autres. A l'inverse, les hautes fréquences sont des zones de contraste, de changement rapide dans les couleurs[2].

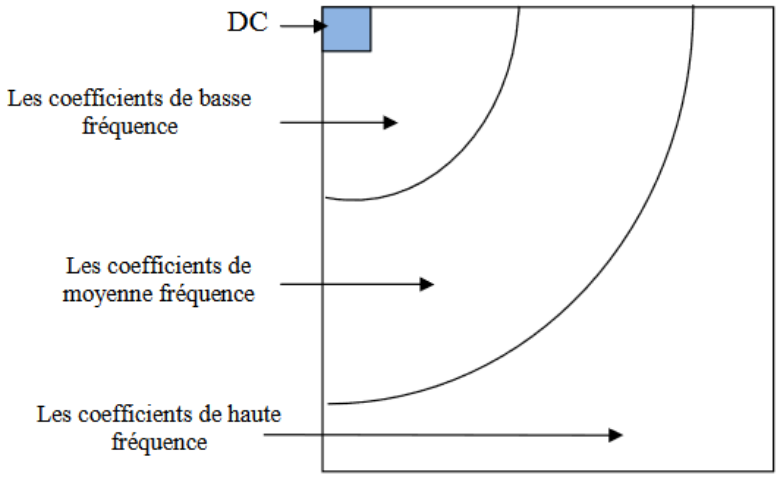


Figure 6 : Les différentes classes de coefficients selon leurs fréquences[2].

c) Quantification :

La quantification a pour objectif d'atténuer les hautes fréquences d'une image qui ont été mis en évidence par la DCT. L'œil humain distingue mal les zones de contrastes (les hautes fréquences) et la quantification va permettre de diminuer l'importance de ces informations superflues.

La technique est simple , Il suffit de diviser notre matrice de fréquence avec la matrice de quantification pour obtenir notre matrice quantifiée.

d) Le codage entropique :

Le codage entropique convertit une série de symboles représentant des éléments de l image en un flux binaire compressé adapté à la transmission ou au stockage.

C'est une technique de compression de données sans perte. D'abord on lit les coefficients de manière « en zigzag ». puis on code par l'algorithme RLE (Run-Length Encoding) pour eliminer la redandance statique,puis on utilise le codage de Huffman .

8. La compression de video (MPEG) :

The Motion Pictures Expert Group (MPEG) a été formé par 'ISO (Organisation internationale de normalisation) pour développer cette norme. Le MPEG a été créé en 1988 pour établir une

norme internationale pour la représentation codée des images animées et du son associé sur les supports de stockage numériques[11].

Une vidéo MPEG est composée d'une séquence de groupe d'images (GOP),Chaque image est divisée en trames et chaque trame est ensuite divisée en macroblocs.

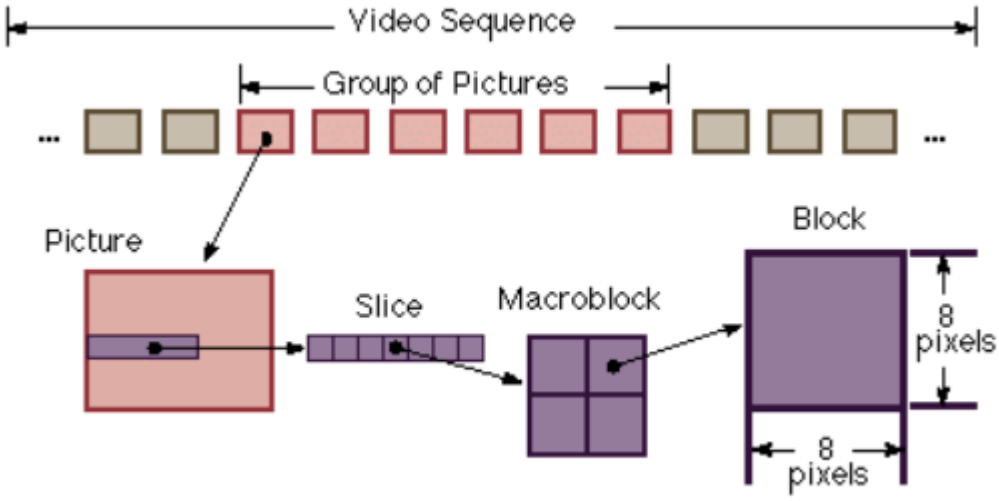


Figure 7: les composants d unevidéo séquence.

La norme MPEG définit spécifiquement trois types d'images [2]:

a) I- trame :

c'est une image intra-codées.en utilisant uniquement les informations présentées dans l'image elle-même, sans aucune référence à d'autres images. Elle est traitée et compressée comme une image fixe.

le taux de compression de la trame Iest le plus faible du MPEG.

b) P-trame :

P- trame sont codées par rapport aux images I ou P précédentes.(coder de manière prédictive).et peuvent également servir de référence de prédiction pour les images B et les futures images P.

c) B-trame :

B- trame sont des images qui utilisent à la fois une image passée et une image future comme référence. Cette technique est appelée prédiction bidirectionnelle. Les images B offrent la plus grande compression puisqu'elles utilisent l'image passée et future comme référence.[3]

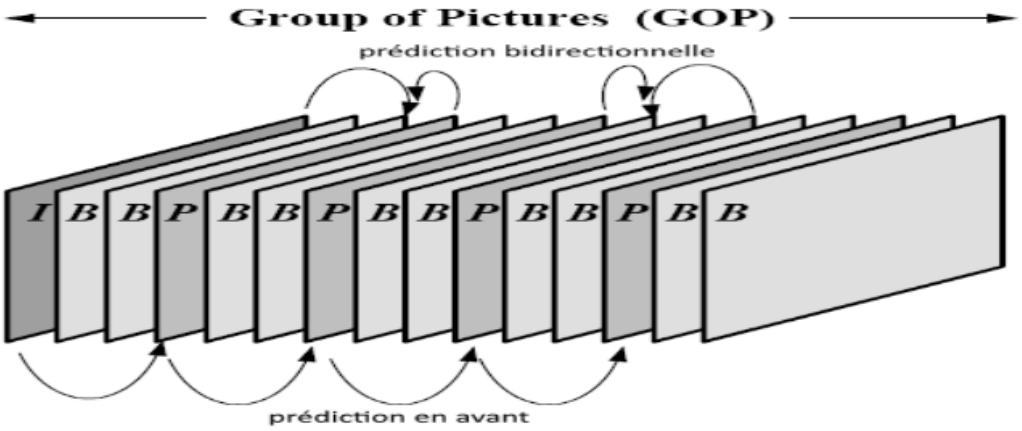


Figure 8:Exemple de groupe d'images avec l'ordre d'affichage.

9. La prédiction :

L'objectif du modèle de prédiction est de réduire la redondance en formant une prédiction des données et en soustrayant cette prédiction des données actuelles. La prédiction peut être formée à partir d'images précédemment codées (prédiction temporelle) ou d'échantillons d'images précédemment codées dans la même image (prédiction spatiale). La Prédiction à partir d'images précédentes est utilisée pour les images P et B[4].

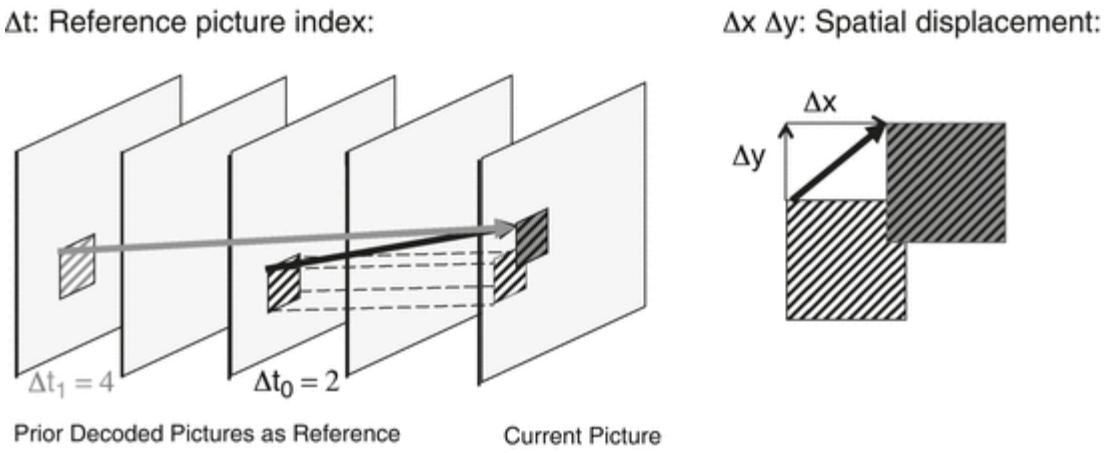


Figure 9:inter Prédiction dans HEVC

10.Conclusion :

Dans ce chapitre, nous avons parlé des images et des vidéos , les méthodes de compression et de codage des vidéos numériques, les normes des compressions vidéo.

Dans le prochain chapitre, nous allons parler de la norme H.264 .

Chapitre II :

La norme H.264.

1. Qu'est-ce que le H.264?

La norme H.264/AVC ou MPEG-4 Part 10, Advanced Video Coding, a été publiée pour la première fois en 2003, par deux organismes de normalisation internes, l'UIT-T et l'ISO/CEI.Elle s'appuie sur les concepts de normes antérieures telles que MPEG-2 et MPEG-4 Visual et offre un meilleur format pour la vidéo compressée qui prend moins de place lorsqu'elle est stockée ou transmise,et une procédure de décodage de cette syntaxe afin de produire une meilleure qualité de la vidéo affichable[6].

2. H.264 codec :

H.264/AVC décrit un ensemble d'outils ou de méthode de compression vidéo. La structure de codage de base de cette norme est similaire à celle des normes précédentes et est communément appelée structure de codage de la transformation .

Le codage de la vidéo s'effectue image par image. Chaque image à coder est d'abord découpée en plusieurs trames(il est également possible d'avoir une trame par image). Les trames sont des unités de codage individuelles dans cette norme par rapport aux normes précédentes car chaque trame est codée indépendamment. Une trame est constituée d'une séquence de macroblocs, Chaque macrobloc 16×16 est divisé en 16×8, 8×16 , 8×8, 8×4, 4×8 et 4×4. La partition 4×4 sous-macrobloc est appelée un bloc.

Un encodeur vidéo H.264 applique trois processus : prédiction, transformation et l'encodage entropique pour produire un flux binaire comprimé [5].

Un décodeur vidéo H.264 exécute les processus complémentaires de décodage entropique, de transformation inverse et de reconstruction pour produire une séquence vidéo décodée.

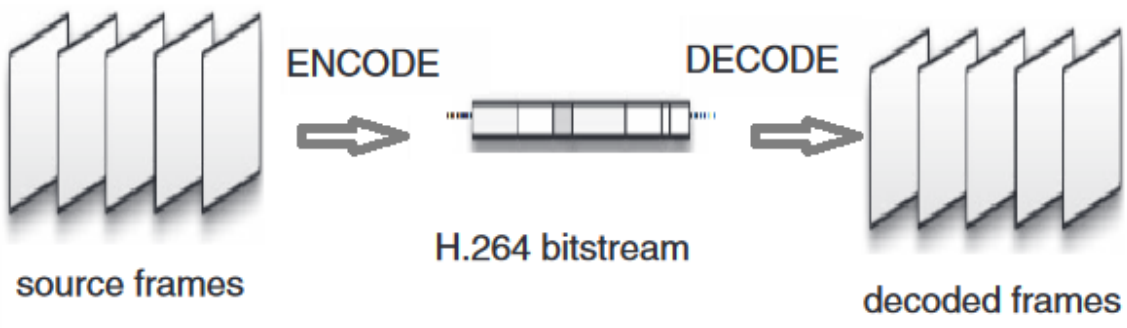


Figure 10:H.264 codec [5]

3. Les étapes de codage de H.264 :

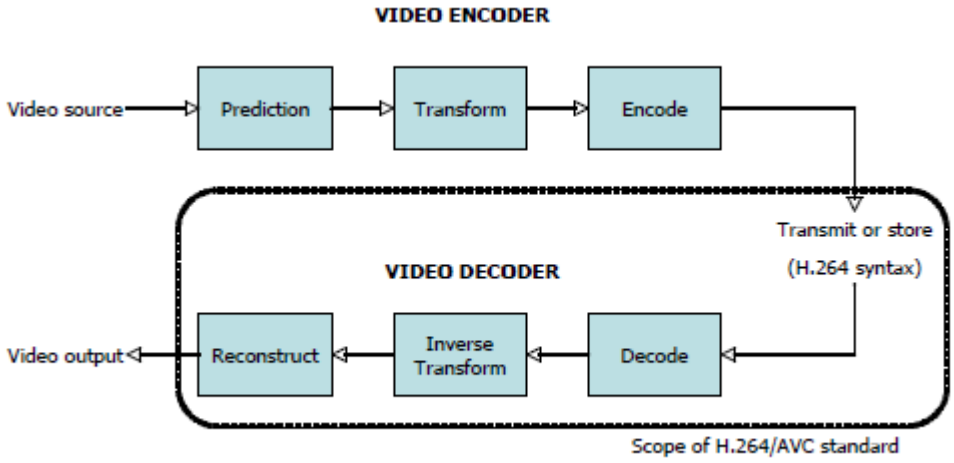


Figure 11: le CODEC H.264

a) Prediction :

Le codeur forme une prédiction du macrobloc actuel sur des macrobloc précédemment codées (buffer), soit à partir de la trame actuelle en utilisant l'intraprédiction, soit à partir d'autres trames qui ont déjà été codées et transmises en utilisant l'interprédiction.La première image de chaque séquence vidéo doit être codée en mode Intra, car elle sert comme une image de référence pour prédire les futures images de la séquence.Les méthodes de prédiction prises en charge par la

norme H.264 sont plus souples que celles des normes précédentes, ce qui permet des prédictions précises et donc une compression vidéo efficace.

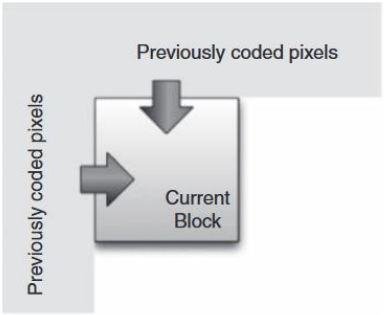


Figure 12: intra prédiction.

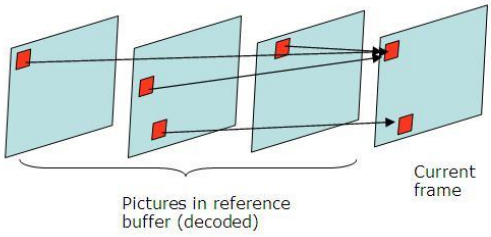


Figure 13: inter prédiction

La prédiction utilise une gamme de tailles de blocs allant de 16×16 à 4×4 pour prédire les pixels de l'image actuelle provenant de régions similaires dans des images codées précédemment. Ces images précédemment codées peuvent se produire avant ou après l'image actuelle dans l'ordre d'affichage[6].

b) La transformation/quantification:

Un bloc d'échantillons est transformé à l'aide d'une transformée en 4×4 ou 8×8, une forme approximative de la transformée en cosinus discrète (DCT). La sortie de la transformée est un bloc de coefficients de transformée, et quantifiée, c'est-à-dire que chaque coefficient est divisé par une valeur entière.

La quantification réduit la précision des coefficients de la transformée en fonction d'un paramètre de quantification (QP).Le réglage de QP à une valeur élevée signifie que plus de coefficients sont réglés à zéro, ce qui entraîne une compression élevée au détriment de la qualité de l'image décodée. Le réglage de QP à une valeur faible signifie qu'il reste plus de coefficients

non nuls après la quantification, ce qui se traduit par une meilleure qualité d'image au niveau du décodeur mais aussi par une compression plus faible[6].

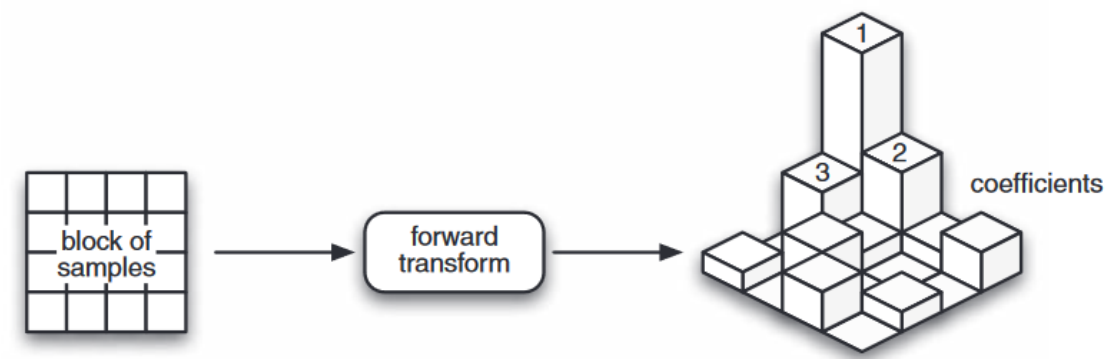


Figure 14: exemple de la phase DCT(la transformée en cosinus discrète)[2]

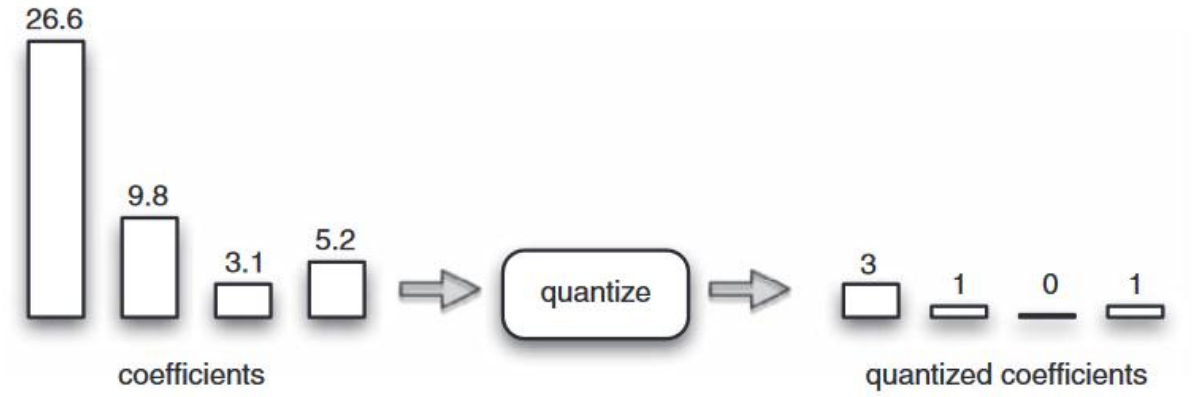


Figure 15: exemple de la phase QUANTIFICATION

c) Le codage entropique :

Comme toutes les normes de compression, la dernière étapes consiste à convertir les données compressées en un flux binaire lisible selon un format normalisé.

Le processus de codage vidéo produit un certain nombre de valeurs qui doivent être codées pour former le flux binaire compressé. Ces valeurs sont les suivantes

- Coefficients de transformation quantifiés
- Informations permettant au décodeur de recréer la prédiction
- Informations sur la séquence vidéo complète.

Ces valeurs ,paramètres et éléments syntaxiques, sont convertis en codes binaires à l'aide de deux modes compresseur : CABAC et CAVLC.

- CABAC : signifie binaire codage arithmétique contextuel. Cette méthode utilise un algorithme très complexe pour maintenir la qualité de l'image, prend donc plus de puissance informatique pour traiter et décoder.
- CAVLC : signifie codage à longueur variable adaptatif au contexte. Celui-ci utilise un algorithme moins complexe que CABAC. Pourtant, il est plus moderne et plus efficace que le CABAC conception entropie plus tôt[2].

4. Les étapes de décodage de H.264 :

Un décodeur vidéo reçoit le flux binaire H.264 compressé, décode chacun des éléments syntaxiques et extrait les coefficients de transformation quantifiés, les informations de prédiction, etc. Ces informations sont ensuite utilisées pour inverser le processus de codage et la transformation inverse et recréer une séquence d'images vidéo.

5. Les profiles de h.264 :

Le standard inclut les trois ensembles de caractéristiques suivants, qui sont appelés des profils, chacun ciblant une classe d'applications précise [5] :

a) Baseline Profile (BP) :

prévu pour les applications qui utilisent peu de ressources, ce profil est très utilisé dans les applications mobiles et de vidéo conférence.

b) Main Profile (MP) :

prévu pour les applicationsqui utilisent grand public de diffusion (TV) et de stockage video.

c) Extended Profile (XP) :

prévu pour la diffusion en flux (streaming) des vidéos, ce profil a des capacités de robustesse à la perte de données et de changement de flux.

6. Conclusion :

En somme, H.264 est le fruit des travaux entre ITU-T et ISO où ellea introduit des nouveaux outils dans tous les étapes,comme CAVLC et CABAC pour le codage entropique.En conséquence, cette norme est adoptée avec succès dans de nombreuses applications mobiles et réseaux pour transmettre des vidéos de différentes tailles.

Le prochain chapitre va jeter lumière sur la protection du contenu informatif de vidéo comprimée.

Chapitre III :

Sécurité de vidéo numérique

1. Introduction :

Ces dernières années, avec le développement des technologies Internet, les technologies vidéo ont été largement utilisées dans la télévision, la communication et le multimédia. sont générées et transmises dans les domaines médical, commercial et militaire, ce qui peut inclure certaines informations sensibles auxquelles les utilisateurs généraux ne devraient pas avoir accès.alors, il faut utiliser des méthodes de cryptage qui puissent protéger la vidéo numérique contre les attaques pendant la transmission.

2. Définition de la cryptographie :

Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant dechiffrer des messages, c'est-à-dir permettant de les rendre inintelligibles sans une action spécifique. On utilise des ensembles de calculs basés sur des règles appelés algorithmes pour transformer les messages de manière difficile à déchiffrer. Ces algorithmes déterministes sont utilisés pour la génération de clés cryptographiques , la signature et la vérification numériques a fin de protéger la confidentialité des données [7].

Crypter : brouiller l'information, la rendre "incompréhensible".

Décrypter :rendre le message compréhensible.

3. Objectifs de sécurité :

a) La confidentialité :

seules les personnes autorisées peuvent avoir accès aux informations. Et Les données sont gardées privées pour ceux qui n'ont pas les qualifications appropriées (credentials)[2].

b) L' intégrité :

Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin. Cet objectif utilise généralement des méthodes de calculs de hachage.

c) Non-répudiation :

L'expéditeur ne peut pas nier ses intentions lors de la transmission ultérieure de l'information.Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues.

d) Authentification :

les utilisateurs doivent prouver leur identité, c.-à-d.assurer que seules les personnes autorisées aient accès aux ressources.(par exemple par le moyen d'un nom utilisateur et un mot de passe qui devra être chifffré) .

4. Les classes de chiffrement :

a) Le chiffrement symetrique :

Également connue sous le nom de chiffrement à clé secrète ou de chiffrement à clé symétrique, le chiffrement à clé symétrique est un système de chiffrage dans lequel les émetteurs et les récepteurs d'un message partagent une clé unique et commune qui est utilisée pour chiffrer et déchiffrer le message. L'utilisation d'un algorithme est également connue sous le nom d'algorithme à clé secrète ou parfois appelé algorithme symétrique.Une clé est un élément d'information (un paramètre) qui détermine la sortie fonctionnelle d'un algorithme ou d'un chiffre cryptographique[17].

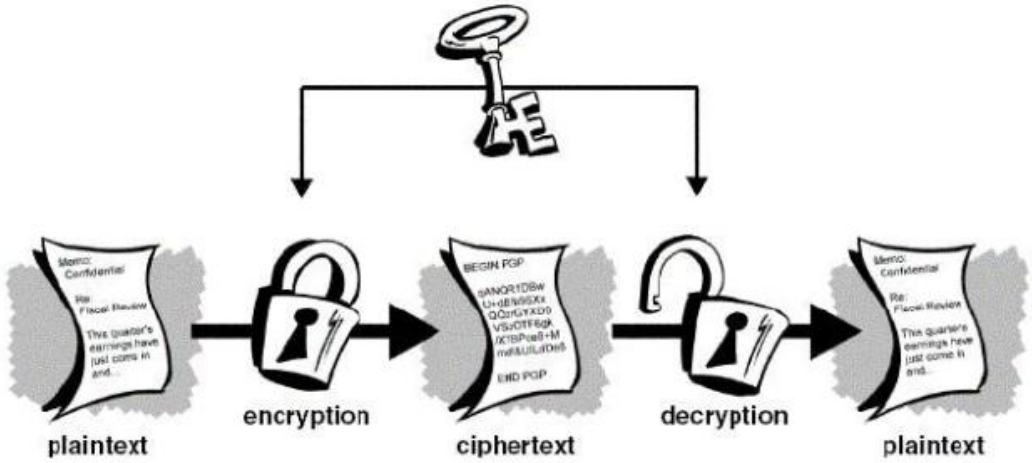


Figure 16: Le schémaChiffrement symétrique .

Les systèmes à clés symétriques sont plus simples et plus rapides ; leur principal inconvénient est que les deux parties doivent échanger la clé de manière sécurisée et la conserver ensuite. La gestion des clés a causé un cauchemar pour les parties utilisant la cryptographie à clé symétrique.

Examples for symmetric key cryptography include AES, DES, and 3DES

b) Le chiffrement asymétrique :

Le chiffrement asymétrique (ou a clé publique) référence à un algorithme cryptographique qui nécessite deux clés différentes, dont l'une est privée et l'autre publique. La clé publique est utilisée pour crypter le message et la clé privée pour le décrypter.

Les deux participants au système de chiffrement asymétrique sont les émetteurs et les récepteurs ; chacun d'eux possède sa propre paire de clés publiques et privées. L'émetteurs obtient d'abord la clé publique du destinataire. Ensuite, le texte en clair - ou le texte ordinaire, lisible - est chiffré par l'expéditeur à l'aide de la clé publique du destinataire ; cela crée un texte chiffré. Le texte chiffré est ensuite envoyé au destinataire, qui le déchiffre avec sa clé privée et le rend lisible en clair[14].

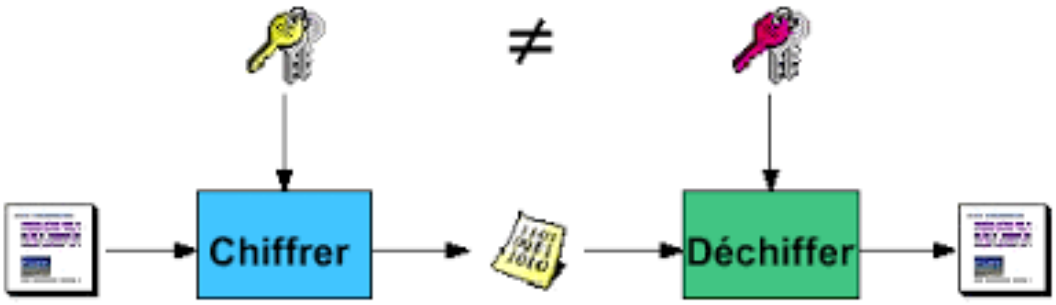


Figure 17: Le schéma Chiffrement asymétrique

c) Fonctions de hachage :

Une fonction de hachage est simplement une fonction qui prend la valeur d'entrée (qui peut être n'importe quelle donnée - nombres, fichiers, etc.), et à partir de cette entrée crée une chaîne de bits de taille fixe déterministe de la valeur d'entrée.

Les fonctions de hachage sont généralement irréversibles (à sens unique), ce qui signifie que vous ne pouvez pas déterminer l'entrée si vous ne connaissez que la sortie - à moins d'essayer toutes les entrées possibles (ce que l'on appelle une attaque par brute force). Un hachage est généralement affiché sous la forme d'un nombre hexadécimal.

5. Modes de chiffrement :

Il existe deux principaux types de chiffrement : le chiffrement par blocs et le chiffrement par flux. Dans le cas du chiffrement par flux le texte en clair est chiffré bit par bit. Dans un chiffrement par blocs, le texte en clair est divisé en blocs d'une longueur déterminée et les bits de chaque bloc sont chiffrés ensemble. Pourcela 4 modes de chiffrement par blocs sont possibles: ECB, CBC, CFB et OFB[3].

a) Le mode ECB (Electronic Code Book) :

Le Electronic Code Book (ECB) est le mode de chiffrement par blocs le plus simple. Dans ce mode, Le message est découpé en blocs, chaque bloc de texte en clair est chiffré séparément. qu'il permet un chiffrement parallèle des différents blocs composant un message.

Mais l'inconvénient de ce mode est que les messages en clair identiques chiffrés avec la même clé permet à un attaquant d'apprendre certaines informations sur le message chiffré.

b) Le mode CBC (Cipher Block Chaining) :

Dans le mode de fonctionnement du chaînage par blocs de chiffres (CBC), un vecteur d'initialisation IV (une valeur aléatoire et publique IV) est combiné par ou exclusif avec le texte en clair avant le cryptage. Pour le premier cycle de chiffrement,. Pour les cycles suivants, il s'agit du texte chiffré du cycle précédent.

Ceci est destiné à résoudre le problème du mode EBC où des blocs de texte en clair identiques créent des blocs de texte chiffré identiques.

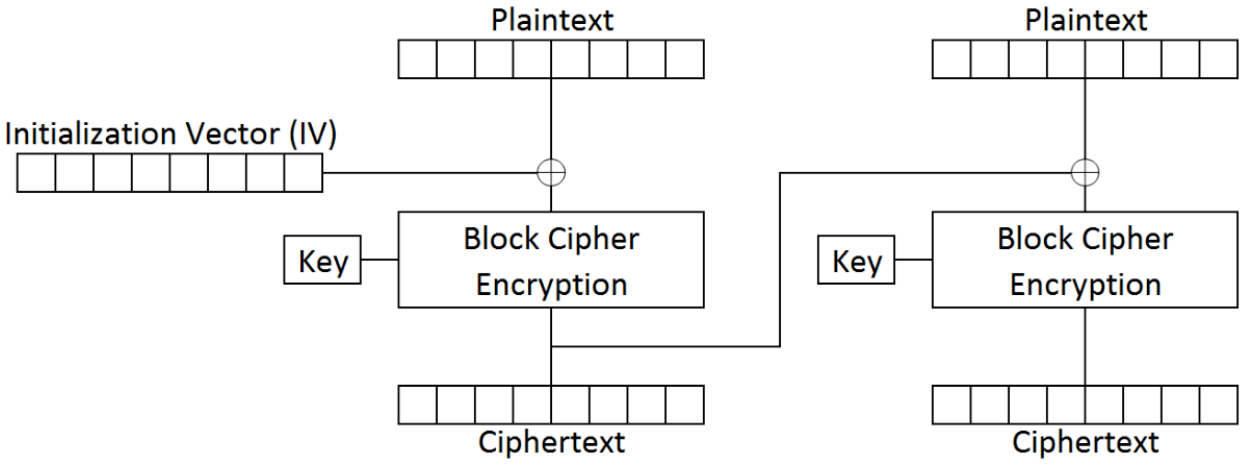


Figure 18:Schéma du chiffrement de mode CBC

c) Le mode CFB(Cipher FeedBack) :

Ce mode est différent des deux précédents ,le texte en clair ne passe jamais par l'algorithme de chiffrement. Au lieu de cela, un vecteur d'initialisation (IV) est chiffré et le résultat est combiné par ou exclusif au texte en clair pour créer le texte chiffré d'un bloc.

d) Le mode OFB (Output FeedBack) :

Dans ce modeest presque identique au mode CFB(Cipher FeedBack).La clé est modifiée à chaque itération et combinée avec la clé suivante.

6. Les algorithmes de chiffrement :

a) Data Encryption Standard (DES) :

DES est un algorithme qui a été le standard de chiffrement symétrique entre 1977 et 2001 par le « National Institute of Standards and Technology (NIST) ».

DES est une implémentation d'un chiffrement Feistel. Il utilise une structure Feistel à 16 ronds. La taille du bloc est de 64 bits. Bien que la longueur de la clé soit de 64 bits, DES a une longueur de clé effective de 56 bits, puisque 8 des 64 bits de la clé ne sont pas utilisés par l'algorithme de chiffrement.

DES a une clé plus petite qui est moins sécurisée et plus lent par rapport à AES a une grande clé secrète comparativement plus sûre et plus rapide. Enplus, le DES a fait l'objet de très nombreuses attaques[14]

b) Advenced Encryption Standard (AES) :

L'Advanced Encryption Standard (AES) est une norme de chiffrage adoptée par le gouvernement américain, est lancé par NIST (National Institute of Standards and Technologies) le 2 octobre2000 pour remplacer Triple DES et DES.

La norme comprend trois blocs de chiffrement, AES-128, AES-192 et AES-256, adoptés à partir d'une plus grande collection publiée à l'origine sous le nom de Rijndael. Chaque chiffre AES a une taille de bloc de 128 bits, avec des tailles de clé de 128, 192 et 256 bits, respectivement.

AES est un système de chiffrement par blocs qui peut être utilisé dans différents modes (ECB ,CBC,CFB…) [15].

c) Le chiffrement XOR :

Le chiffrement XOR est une méthode utilisée pour chiffrer les données ,c'est-à-dire en générant des clés de chiffrement aléatoires pour qu'elles correspondent à la bonne clé.

Le concept de l'implémentation consiste à définir d'abord la clé de chiffrage XOR et ensuite à effectuer une opération XOR des caractères de la chaîne avec cette clé que vous voulez crypter. Pour décrypter les caractères cryptés, nous devons à nouveau effectuer une opération XOR avec la clé définie. [17]

7. Sécurité de vidéo numérique :

En comparaison avec la communication textuelle, la communication vidéo se caractérise par un certain nombre de caractéristiques particulières, telles que la grande taille des données, les exigences en temps réel, l'utilisation de codecs vidéo standard, les formats de compression de données standard et les exigences de sécurité spécifiques à l'application[19].

8. Classificationde chiffrement des vidéos :

Il existe deux types principauxpour le chiffrement vidéo:chiffrement total et sélectif.

a) Le chiffrement total (full encryption) :

Ce type de cryptage consiste à chiffrer toutes les données vidéo. Le flux vidéo (séquence de bits) est traité comme des données plaintext, et chaque octet est crypté à l'aide d'algorithmes de cryptage standard comme DES, RC5 ou AES, etc.Cette méthode est largement utilisée pour la sécurité des images,mais , il est rarement utilisé pour le chiffrement vidéo, car s'il est appliqué pour chiffrer chaque image séparément, il va entraîner une augmentation du volume de la vidéo cryptée.[19]

b) Le chiffrement sélectif (selective encryption) :

Il offre une sécurité plus rapide car il ne crypte qu'une partie sélectionnée d'un flux de bits, ce qui permet de crypter sélectivement les octets qui contient des informations sensibles.Les données chiffrées sont sélectionnées selon des critères et des conditions très variés pour protéger la confidentialité de la vidéo.

Le chiffrement sélectif est appliqué independent ou durant la compression[2].

9. Chiffrementet compression vidéo :

la relation entre la compression et le chiffrement estdéfinitpardeux classes primaires : Chiffrement indépendant de compression ou Chiffrement durant de compression.

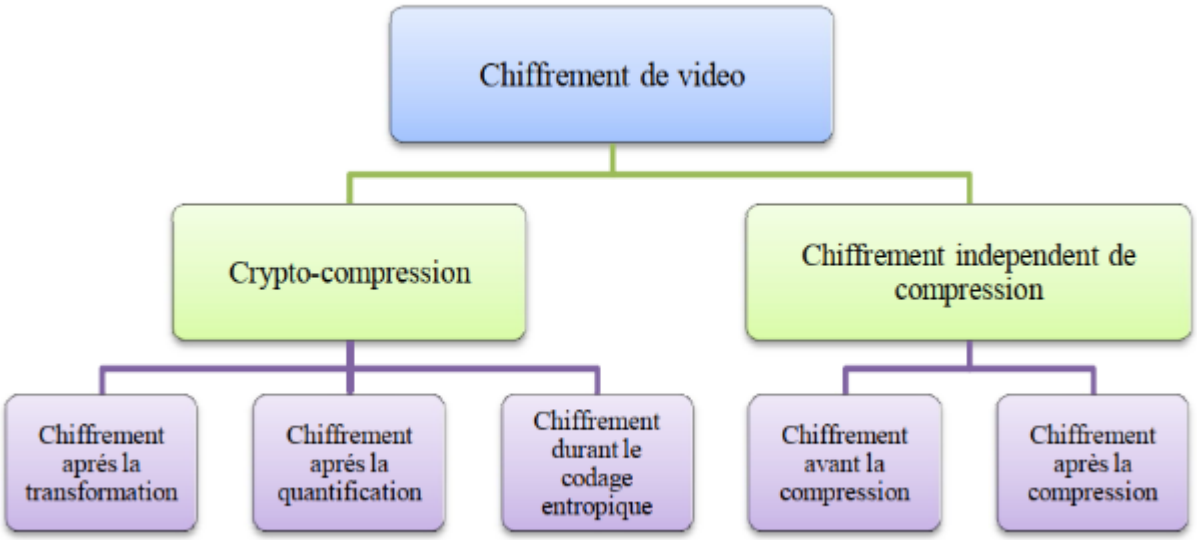


Figure 19:Taxonomie des techniques de chiffrement de vidéo numérique.

a) Chiffrement indépendant de compression :

Le cryptage des flux vidéo peut se faire avant ou après la compression, mais cette méthode pose des problèmes de compatibilité avec les codecs. Lorsque la vidéo est cryptée avant la

compression, le codec est portable mais la taille des données augmente. Lorsque la vidéo est chiffrée après la compression, elle n'est pas, par nature, compatible avec les codecs..

Chiffrement avant la compression :

les données avant la compression contiennent beaucoup de redondance, Les algorithmes de compression sont prévus pour réduire ce redondance .

si on utilise les opérations cryptographiques avant compression seront beaucoup moins de redondance pour comprimer .

les algorithmes du chiffrement sont rarement rendus effectifs avant compression. Parmi les algorithmes de chiffrement se plaçant avant la compression ; l'approche de Pazarci-Dipc et l'approche de chiffrement a base de préservation de corrélation de vidéo CPEV

Chiffrement après la compression :

Le chiffrement naïf de la vidéo compressée peut affecter le décodage de la vidéo cryptée, car le format de flux binaire ne sera pas conforme avec la norme de codage convenue[22].

Meyer et Gadegast [3]ont proposé un chiffrement sélectif pour la norme MPEG 1en 1995. Les parties sélectionnées pour la protection sont chiffrées par des algorithmes de chiffrement conventionnels. Mais Malheureusement, le format deflux binaire crypté n'est pas conforme à la syntaxe approuvée de la norme H.264.

b) Chiffrement durant la compression(crypto-compression) :

Le cryptage peut également se produire en même temps que la compression. Cette méthode dépend du codec et réduit le temps de traitement global, mais elle est moins sûre et peut être coûteuse en termes de traitement[24].

Chiffrement après la transformation :

Les données à chiffrer après la transformation fréquentielle de l'erreur résiduellesont les amplitudes et les signes des coefficients. Chaquenorme de codage dispose deson propre transformée appliquée. Le plus populaire est la transformée de DCT et ses améliorations.

Le chiffrement des coefficients de DCT est moins préféré, car les amplitudes seront modifiées après la quantification qui est une fonction irréversible[2].

Chiffrement après la quantification :

La quantification est l'étape qui permet la réduction de l'espace de coefficients. Ces derniers seront balayés et parcourus selon un mode de balayage. Le mode en zigzag est le plus populaire car il commence parles coefficients de basses fréquences, et il termine parles coefficients à hautes fréquences dont l'ordre de chaque QTCest déterminé selon la norme de codage adoptée. Les données possibles à chiffrer sont: les amplitudes et les signes de QTCs, et aussi l'ordre de QTCs.

Chiffrement durant le codage entropique :

Après la sortie et la standardisation de chaque norme de codage vidéo, lapréservation de la taille de flux binaire crypté sans augmentation, et avoir un formatconforme décodable selon la syntaxe de la norme, occupe une préoccupation majeure pour la communauté cryptographique, car elle représente un défi réel à surmonter.Elle repose sur l'étude de la décidabilité des éléments syntaxiques après le chiffrement. Le choix de ces éléments syntaxiques et sa protection par un chiffrement sélectif sont des étapes communes suivies par la majorité d'approches de chiffrement durant le codage entropique existantes dans la littérature scientifique

10.Conclusion

Nous avons vu dans ce chapitre, une vue d'ensemble des différentes méthodes de cryptographie actuellement connues a été présentée. Les deux différents types de méthodes de cryptage (cryptage à clé symétrique et cryptage à clé asymétrique).De plus, les algorithmes de cryptage.

Chapitre IV :

Approche proposée et implimentation

1. Introduction:

Le chiffrement de video peut se faire avant la compression, durant la compression, ou aprés la compression où la video peut etre chiffrée entierement par une approche de chiffrement total, ou partielement par une approche de chiffrement selectif. Dans ce chapitre, nous allons presenter une approche de chiffrement selectif durant la compression des données frequentielles de la video. Ensuite, nous allons evaluer les resultats de l'approche proposée en terme de metriques objectifs et/ou subjectifs.

2. Presentation de l'approche proposée :

L'encodage H.264 transforme en video comprimé une video presumée brute representée en format YC_BC_R où Y represnte la luminance. L'encodage passe evidement par la prédiction, transformation, quantification et l'encodage entropique tandis que le décodage se passe par les memes opérations mais en sens inverse. Notre approche de crypto-compression (figure 20) se deroule entre l'etape de quantification par le chiffrement de coefficients quantifiés bien selectionés et le codage entropique tandis que le déchiffrement se fait entre l'etape de decodage entropique et la déquantification (quantification inverse).

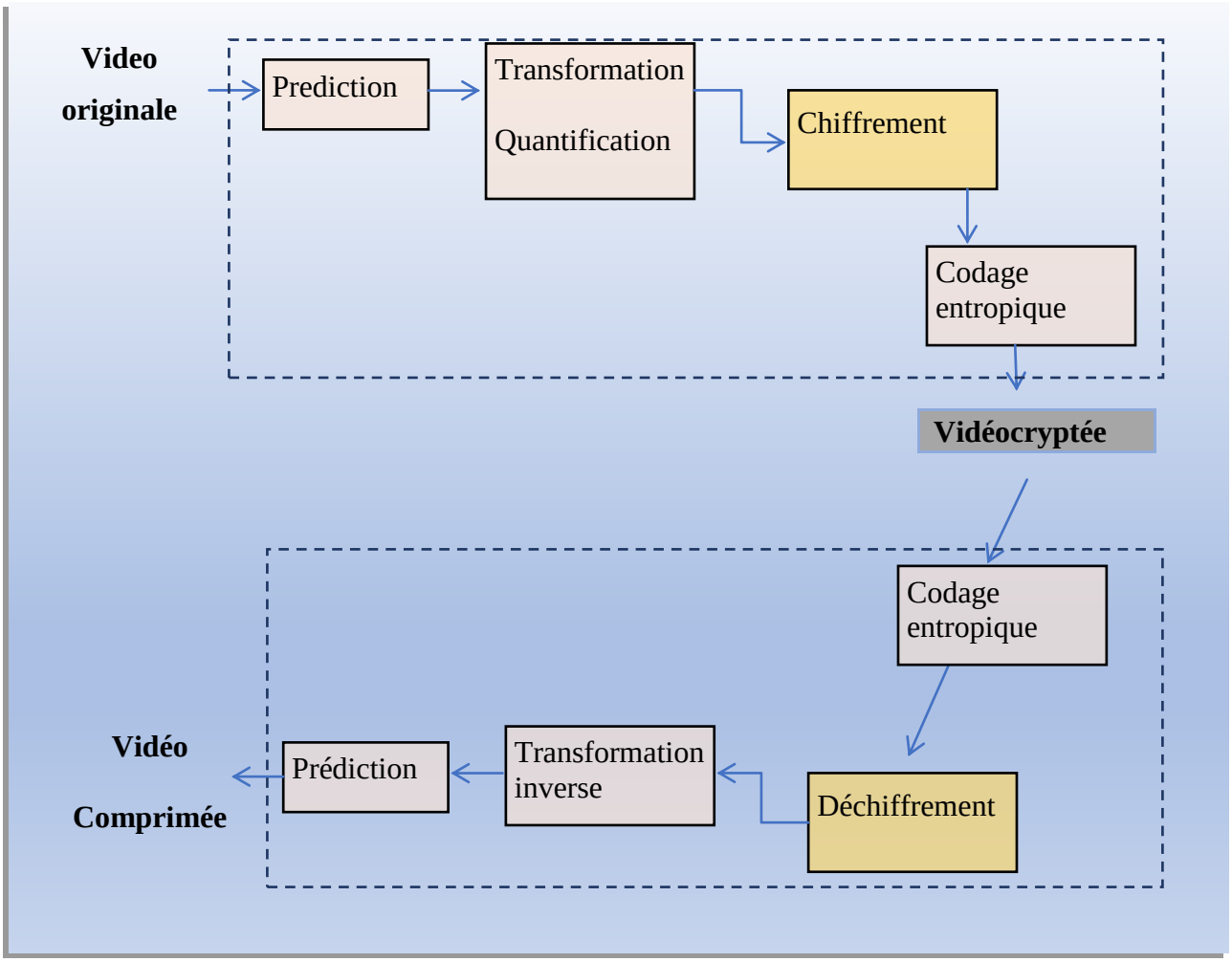


Figure 20:les étapes à suivre de codage au decodage avec le chiffrement/dechiffrement de notre approche proposée.

3. Chiffrement :

Chaque trame de la video à coder en H.264 est representée en système colerimetrique YCbCr où les composantes couleur de ce système sont décorrelées.Comme le système visuel humain est plus sensible aux variations de luminance qu'aux celles de chrominances, les données choisis pour le chiffrements sont celles de luminance. Chaque trame est decomposée en macrobloc de 16×16 pixeles avant son passage à l'etape de prediction. Cette derniere partitionne chaque macrobloc en partitions variée (4×4, 4×8, 8×4, 8×8, 16×8, 8×16, 16×16) afin de trouver l'erreur residuelle optimale.Chaque partition predite qui représente ainsi l'erreur residuelle est decomposée ensuite en bloc de 4×4 elements[18].

La transformée entière (TI) opère sur des blocs de données résiduelles 4x4 après la prédiction. La transformation est basée sur la DCT, mais avec quelques différences fondamentales :

a) Elle est une transformée entière (toutes les opérations peuvent être effectuées avec une arithmétique entière, sans perte de précision).
b) elle est plus simple et requiert seulement des additions et des décalages binaires (bit shift).
c) L'ensemble du processus de transformation peut être effectué en utilisant une arithmétique entière sur 16-bit et seulement une multiplication par coefficient, sans aucune perte de précision.

Chaque bloc de l'erreur residuelle *X* (données spatialles) est transformée en bloc de coefficients frequentiels *Y* suivant la formule suivante :

$Y = AXA^T$ (IV.1)

Sachant que $A = \begin{vmatrix} 1 & 1 & 1 & 1/2 \\ 1 & 1/2 & -1 & -1 \\ 1 & -1/2 & -1 & 1 \\ 1 & -2 & 2 & -1 \end{vmatrix}$ (IV.2)

Apres la transformation, *Y* est soumis à une etape de quantification pour eliminer des basses frequences selon un parametre appelé le pas de quantification *QP* variant de 0 à 52. Une valeur minimale de ce dernier signifie une baisse compression et une qualité visuelle forte tandis que une valeur superieur signifie une forte compression avec une degradation dans le rendu visuel.

Après la quantification, le nouveau bloc de coefficients quantifiés $\{qtc_{i,j}, i = 1 \dots 4, j = 1 \dots 4\}$est transformé en flux binaire (bits) à travers le codage entropique. H.264 utilise la prediction pour eliminer la redondance spatiale, la quantification pour éliminer la redondance frequentielle, et aussi le codage entropique pour un codage optimal du flux binaire engendrant ainsi le fichier binaire de la video compressée.

Le codeur entropique encode les amplitudes (valeurs absolus) $|qtc_{ij}|$et les signes de coefficients quantifiés separement. Aussi, les amplitudes sont classés en trois classes : les zeros $|qtc_{ij}| = 0$, les uns où $|qtc_{ij}| = 1$ et les autres où $|qtc_{ij}| \geq 2$.

Les signes des amplitudes sont regroupés en bloc avec le remplacment de -1 par 0 pour les coefficients negatifs.

Afin de ne pas alterer grandement la taille de la video compressée, nous avons decider de chiffrer seulement les signes et les amplitudes $|qtc_{ij}| \geq 2$, car le chiffrement des zeros $|qtc_{ij}| = 0$ permet d'augmenter la taille et de perdre le resultat estompé de la quantification. De meme, le chiffrement des uns $|qtc_{ij}| = 1$ pourra aussi augmenter la taille de flux binaire de la video compressée.

La figure (21) suivante illustre l'etape de chiffrement qui se deroule entre l'etape de quantification et l'etape de codage entropique alors, la figure illustre les données choisies pour le chiffrement.

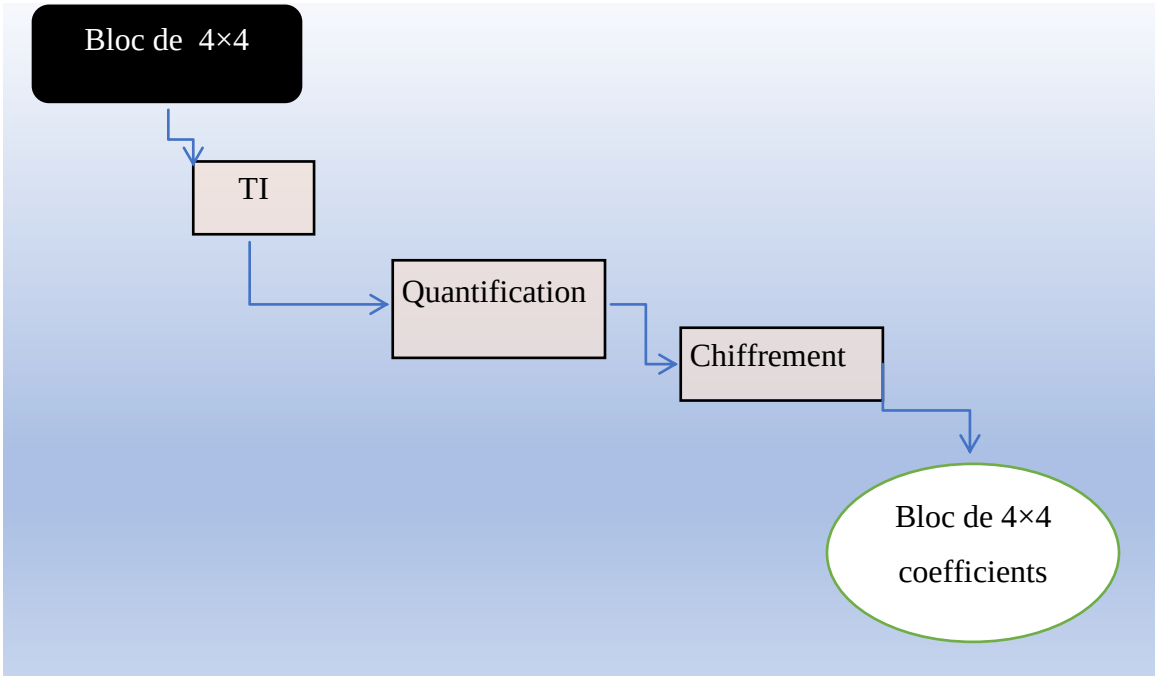


Figure 21:chiffrement d'un bloc de 4×4 de données residuelles.

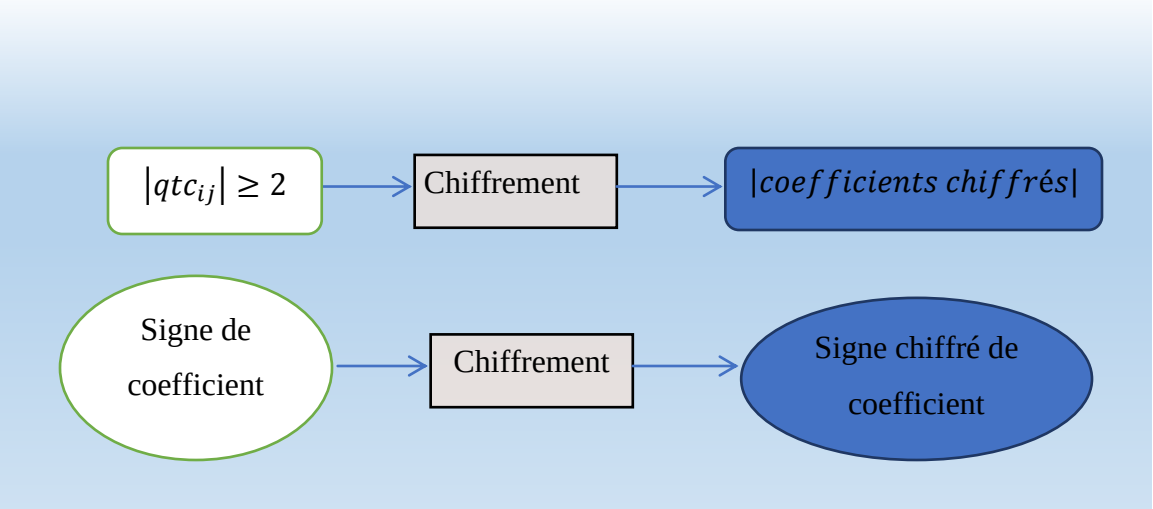


Figure 22:les données residuelles à chiffré.

L'algorithme utilisé pour le chiffrement des amplitudes est decrit comme suit :

Données	bloc de 4×4 données residuelles quantifiées $\{qtc_{i,j}, i = 1 \dots 4, j = 1 \dots 4\}$ Clé de chiffrement (tableau de 4×4×8 bits).
Resultats	bloc de 4×4 données residuelles chiffrées$\{qtce_{i,j}, i = 1 \dots 4, j = 1 \dots 4\}$
Algorithme	Pour i allant de 1 :4 Pourjallant de 1 :4 **Si** ($\|qtc_{ij}\| \geq 2$) **alors** $\|qtce_{ij}\| \leftarrow \|qtc_{ij}\| \oplus clé_{ij}+2$ Fin si Fin pour Fin pour

Tableau 1: L'algorithme utilisé pour le chiffrement des amplitudes

Sachant que $\oplus$ l'operation XOR [17] de ou exlusif.

Le bloc de signes est un tableau qui contient seulement les signes de coefficients non nuls, pour cela, l'algorithme de chiffrement pourra etre decrit comme suit :

Données	bloc de 4×4 signes. Clé de chiffrement (tableau de 4×4×1 bits).
Resultats	bloc de 4×4 signes chiffrés.
Algorithme	Pour i allant de 1 :4 Pour j allant de 1 :4 **Si** ($\lvert qtc_{ij} \rvert \geq 1$) **alors** $signe(qtce_{ij}) \leftarrow signe(qtc_{ij}) \oplus clé_{ij}$ Fin si Fin pour Fin pour

Tableau 2: l'algorithme de chiffrement les signes de coefficients non nuls

4. Déchiffrement :

Le dechiffrement est l'operation de restitution de la video clair comprimée a partir de la video chiffrée comprimée. Par consequent, les données a dechiffrer sont seulement les signes des amplitudes non nuls et les coefficients ayant la condition $\lvert qtce_{ij} \rvert \geq 2$ où son chiffrement est decrit dans les algorithmes suivants :

Données	Clé de chiffrement (tableau de 4×4×8 bits). bloc de 4×4 données residuelles chiffrées$\{qtce_{i,j}, i = 1 \dots 4, j = 1 \dots 4\}$
Resultats	bloc de 4×4 données residuelles claires$\{qtc_{i,j}, i = 1 \dots 4, j = 1 \dots 4\}$

Algorithme	Pour i allant de 1 :4 Pourjallant de 1 :4 **Si** ($\lvert qtce_{ij} \rvert \geq 2$) **alors** $\lvert qtc_{ij} \rvert \leftarrow (\lvert qtce_{ij} \rvert - 2) \oplus clé_{ij}$ Fin si Fin pour Fin pour

Tableau 3: L'algorithme utilisé pour le déchiffrement des amplitudes

Données	bloc de 4×4 signes chiffrés. Clé de chiffrement (tableau de 4×4×1 bits).
Resultats	bloc de 4×4 signes chiffrés.
Algorithme	Pour i allant de 1 :4 Pour j allant de 1 :4 **Si** ($\lvert qtce_{ij} \rvert \geq 1$) **alors** $signe(qtc_{ij}) \leftarrow signe(qtce_{ij}) \oplus clé_{ij}$ Fin si Fin pour Fin pour

Tableau 4: l'algorithme de déchiffrement les signes de coefficients non nuls

5. Resultats experimentaux :

a) Definition de matlab :

MATLAB (matrix laboratoire) est un langage de programmation et un environnement de développement de quatrième génération; Il est utilisé à des fins de calcul numérique. Développé par MATHWORKS, MATLAB permet la manipulation de matrices, l'affichage de courbes et de

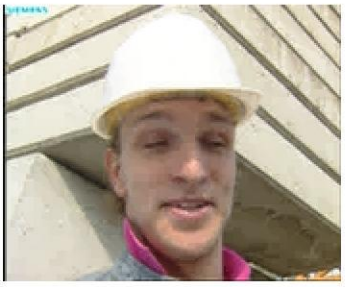
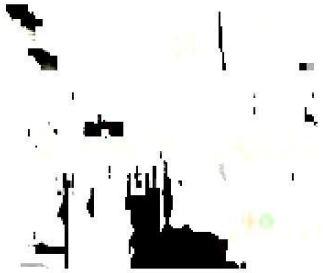
données, la mise en œuvre d'algorithmes, la création d'interfaces utilisateur et peut interagir avec d'autres langages tels que C, C ++, Java. Les utilisateurs de MATLAB (près d'un million d'utilisateurs en 2004) proviennent d'horizons très différents tels que l'ingénierie, la science et l'économie dans des contextes industriels et de recherche. MATLAB peut être utilisé seul ou en combinaison avec des boîtes à outil.[25]

b) Implémentation et resultat:

Nous avons implementé notre approche de crypto-compression en l'integrant dans la bibliothéque H.264 Baseline Codec v2 [21]. Ce codeur permet de lire une video en format YUV et d'extraire aussi les composantes de luminance et de chrominances appropriées et d'executer aussi les operations de prediction, transformation, quantification et le codage entropique.Cependant, ce codeur encode seulement la composante de luminance où chaque groupe d'images est composé d'une trame intra suivi de trame inter predite trame de type P.

Figure 23:une image intra claire et autre chiffrée selon notre approche..

La figure (23) et (24) respectivement illlustrent la trame intra claire (sans chiffrement) et chiffrée pour differentes sequences videos pour un pas de quantification QP=30:

Sequence	Image claire	Image chiffrée
foreman		
akiyo		
bus		

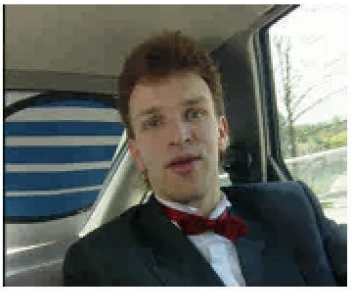
carphone		
miss-america		
soccer		

Figure 24:image intra claire et chiffrée selon notre approche pour un pas QP=30.

Nous remarquons que la qualité visuelle est fortement diminuée où le contenu visuel est approximativement effacé. Comme nous avons chiffré seulement des données residuelles et non les modes de prediction, les trames cryptées conservent les regions de trames en claire.

L'evalutation de la qualité visuelle de l'approche proposée est faite par des mesures objectifs comme le PSNR et SSIM.

Le PSNR :

Rapport signal sur bruit crête (PSNR) mesure la performance de la fidélité visuelle, puisqu'elle est proportionnelle à la qualité, une faible valeur de PSNR signifie qu'une mauvaise qualité visuelle est obtenue tandis que une valeur superieure signifie que la qualité visuelle est en bonne état. Le PSNR se calcule a travers la formule suivante [3]:

$$PSNR = 10 \log_{10} \frac{255^2}{EQM} \quad \text{(IV.3)}$$

Sachant EQM represente la distorsion engendré entre l'image originale et l'image a mesurer et peut etre calculé par :

$$EQM = 1/M.N \sum_{n=1}^{N} \sum_{m=1}^{M} \left(I_{originale}(m,n) - I_{compresse}(m,n) \right)^2 \quad \text{(IV.4)}$$

Nous avons calculé le PSNR pour differentes pas de quantification et nous avons obtenu des basses valeures pour QP=18 (qualité basse de compression), QP= 28 (qualité moyenne de compression) et QP=40 (qualité forte de compression) pour les sequences chiffrés[24].

sequence	Codage sans chiffrement	Codage avec chiffrement
foreman	45.4101	5.4371
bus	44.7469	12.0427
soccer	44.9347	8.7502
Carphone	45.8469	9.6744
akiyo	46.7197	11.0297

Tableau 5: Calcul de PSNR pour QP=18.

sequence	Codage sans chiffrement	Codage avec chiffrement
foreman	37.6349	7.8271
bus	35.5992	14.7047
soccer	36.6026	12.8779
Carphone	38.1224	10.5349
akiyo	39.2322	14.7110

Tableau 6: Calcul de PSNR pour QP=28.

sequence	Codage sans chiffrement	Codage avec chiffrement
foreman	29.6008	6.8015
bus	26.3156	9.1792
soccer	29.3814	7.7514
Carphone	29.6066	7.1757
akiyo	30.8785	8.0863

Tableau 7: Calcul de PSNR pour QP=40.

Le SSIM (Structural Similarity Index):

L'indice de similarité structurelle (SSIM) est une mesure perceptuelle qui quantifie la dégradation de la qualité des images causée par des traitements tels que la compression des données, chiffrement ou par des pertes de transmission de données. C'est une mesure de référence complète qui nécessite deux images de la même capture d'image - une image de référence et une image traitée. L'image traitée est généralement compressée.

la formule de calculde la méthode c'est :

$$SSIM(x,y) = \left(\frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu_x^2+\mu_y^2+c1)(\sigma_x^2+\sigma_y^2+c2)}\right) \text{(IV.5)}$$

μ_x est la moyenne de x.

μ_y est la moyenne de y.

σ_x^2 est la variance de x.

σ_y^2 est la variance de y.

σ_{xy} est la covariance de x et y.

C1=$(K_1L)^2$; avec k1=0.01 et L: nombre d'échelons de Luminance.

C2=$(K_2L)^2$; avec k2=0.03 et L: nombre d'échelons de Luminance

sequence	Codage sans chiffrement	Codage avec chiffrement
foreman	0.989	0.0014
bus	0.986	0.0012
soccer	0.988	0.0023
Carphone	0.991	0.0052
akiyo	0.999	0.0019

Tableau 8.: Calcul de SSIM pour QP=24

6. Conclusion:

Dans ce chapitre nous avons présenté notre approche, qui dépend sur le chiffrement sélectif pour la norme de codage vidéo H.264/AVC.

Nous avons utilisé l'algorithme de cryptage symétrique XOR pour crypter les coefficients quantifiés, Enfin, nous avons discuté des résultats obtenus.

CONCLUSION GÉNÉRALE

Avec le développement des technologies informatiques et de l'internet, les données multimédia sont devenues la méthode la plus pratique pour la formation sensible.

La norme H.264 est caractérisée par plusieurs nouveaux outils introduite dans les différentes phases de codage/décodage. En prédiction, cette norme est renforcée par plusieurs modes d'intra-prédiction. La transformée entière qui est une version améliorée de la transformée en cosinus discrets est introduite pour éviter les problèmes d'arrondissement. Le codage entropique est caractérisé par l'introduction des codeurs adaptatifs aux contextes comme CAVLC et CABAC.

Au cours de ce mémoire, un algorithme de cryptage par une approche de chiffrement sélectif pour les vidéos compressées en H.264 a été proposé pour échanger en toute sécurité des vidéos confidentielles.

Le but principal de ce chiffrement est de maintenir un équilibre entre sécurité et temps de calcul .

Finalement, Les résultats expérimentaux montrent que notre approche dispose un niveau élevé de sécurité et processus plus rapide pour le cryptage et le décryptage.

Bibliographie

[1] S.Ismahane,Thése Doctorat, Sécurisation évolutionnaire du transfert d'images, 2012.

[2] O. Mokhtar, thèse Doctorat, sécurité et compression de l'information multimédia, 2015.

[3] C. BOUBAKEUR, mémoire master, CHIFFREMENT VIDEO NUMERIQUE, 2019.

[4] Chroma subsampling,https://www.rtings.com/tv/learn/chroma-subsampling,2019

[5] Iain E. Richardson, livre, THE H.264 ADVANCED VIDEO COMPRESSION STANDARD Second Edition,2010.

[6] A Survey of H.264 AVC/SVC Encryption-Part I , 2012.

[7] Dr. S.R. Ely (BBC), MPEG Video coding-A simple Introduction in EBU Technical Review Winter 1995 Ely.

[8] Cryptographiequantique,https://fr.wikipedia.org/wiki/Cryptographie_quantique,

[9] http://igm.univ-mlv.fr/~dr/XPOSE2013/La_compression_de_donnees/types.html

[10] wikipedia,https://fr.wikipedia.org/wiki/MATLAB, consulté le 13 02 2019.

[11] A.Puria, X.Chen ,A.Luthra, Video coding using the H.264/MPEG-4 AVC compression standard,SienceDirect, pp. 1701-1713, 1993.

[12] K. Panusopone, X. Chen, R. Eifrig, A. Luthra,Coding tools in MPEG-4 interlaced video, IEEETrans. Circuits Systems Video Technol.2000

[13] J shah and Dr. V Saxena,Video Encryption: A Survey, 2011

[14] S Bahaettđn , an image encryption algorithm robust to post- encryption bitrate conversion

[15] N.GAMA,Thése Doctorat,Géométrie des nombres et cryptanalyse de NTRU, 2008.

[16] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/01-Introduction%20to%20Cryptography.pdf

[17] Cryptographie , https://fr.wikipedia.org/wiki/Cryptographie.

[18] Dépt S.R.C. - I.U.T. de Marne la Vallée,Vidéo numérique

[19] S. Lian, Multimedia Content Encryption: Techniques and Application, CRC, 2008

[20] https://www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdf

[21] https://www.mathworks.com/matlabcentral/fileexchange/55901-h-264-baseline-codec-v2

[22] F.Liu, H.Koenig, A survey of video encryption algorithms, Sience Direct, vol. Volume 29, n° 1Issue 1, pp. 3-15, February 2010.

[23] A.Chadha, S.Mallik, A.Chadha, R.Johar, M. ManiRoja,Dual-Layer Video Encryption using RSA Algorithm, IJCA, vol. Volume 116 –No. 1, pp. 33-40, 2015.

[24] Mokhtar Ouamri and Kamel Mohamed Faraoun, ‘’New Compliant Scheme for Selective Encryption of HEVC/H.265 Videos’’, Journal of Information Processing Systems (ISSN: 1976-913X(Print), ISSN: 2092-805X(Online)) .

[25] Adrian Biran et Moshe Breiner,"MATLAB pour l'ingénieur : Versions 6 et 7", Pearson Education, 2004 (ISBN 2744070254).